## REMARKS

Claims 1-20 are pending. Claims 1 and 7 have been amended. Claims 1-20 remain in this application.

The Specification has been amended to reflect the current status of referenced co-pending applications and to correct minor typographical errors. In addition, reference numerals in FIGURE 2 have been corrected to conform to the written specification. Support can be found on page 9, first paragraph. No new matter has been entered. Approval of the corrections to FIGURE 2 is requested.

A Requirement for Information pursuant to 37 C.F.R. §1.105 was included with the Office action. In response, an Information Disclosure Statement citing the requested art reference is being submitted with this paper. Withdrawal of the Requirement for Information is requested. Acknowledgement of the Information Disclosure Statements and entry of the cited art references on the record are also requested.

Claims 1-12 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Claims 1 and 7 have been amended. No claim has been amended in response to the 35 U.S.C. 103(a) rejections. Withdrawal of the rejection for indefiniteness is respectfully requested.

Claims 1-11 stand rejected under 35 U.S.C. §103(a) as being obvious over C.A. Huegen, "The Latest in Denial of Service Attacks: 'Smurfing' Description and Information to Minimize Effects," ("Huegen"), in view of CERT Advisory CA-1996-21, TCP SYN Flooding and IP Spoofing Attacks ("CERT Advisory"). Applicant traverses the rejection. To establish a *prima facie* case of obviousness: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or combine the reference teachings; (2) there must be a reasonable expectation of success; and (3) the combined references must teach or suggest all the claim limitations. MPEP §2143.

Huegen discloses various techniques for avoiding or minimizing the effects of "smurf" and "fraggle" attacks on computer networks. Huegen further discloses that such attacks make use of ICMP echo requests and the broadcast

capability provided by network routers. (*Id.*) By substituting the intended victim's address as the supposed source address of the echo request, the broadcast capability of the network receiving the echo requests multiplies the requests many times over and returns multiple echoes to the victim via the spoofed address. (*Id.*) This duplication of requests ties up the resources of both the intermediary, that is, broadcast devices, and the victim device receiving the multiple echo replies.

Huegen discloses three principal approaches to avoiding or minimizing the effects of "smurf" or "fraggle" attacks. First, Huegen teaches that networks can take steps to avoid being used as the source of such attacks (page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS). Specifically, Huegen teaches that routers can avoid sending packets with spoofed addresses by checking the source address of a packet against a routing table to ensure that the return path is through the interface through which the packet was received. (*Id.*, para. 4.) Second, Huegen teaches that networks can take steps to avoid being intermediaries in such attacks (pages 2-5, HOW TO STOP BEING AN INTERMEDIARY). Specifically, Huegen recommends that routers be set so as to deny the forwarding and receipt of directed broadcasts. (*Id.* at page 3, para. 3.) This recommendation is based on Huegen's belief that such behavior is not currently needed. (*Id.*) Finally, Huegen teaches that potential victims of "smurf" and "fraggle" attacks can take steps to avoid being victimized (pages 6-8, INFORMATION FOR VICTIMS AND HOW TO SUPPRESS ATTACKS). Specifically, Huegen teaches that various forms of filtering can be used to limit the number of packets entering a network at the network's border. (*Id.*) This filtration can be achieved by handling packets at the interrupt level to avoid using process-level time. (*Id.* at page 6, para. 5.) Or, a committed access rate can be used to limit the rate at which echo and echo-reply traffic is handled at network borders. (*Id.* at page 7, para. 3).

CERT Advisory discloses the basic technique and principles behind SYN flooding attacks on computer networks and further discloses a partial solution to the problem (page 1, para. 4). CERT Advisory teaches that SYN flooding attacks exploit the steps used in establishing a TCP connection and, in particular, uses IP

spoofing to trick servers into sending SYN-ACK messages to non-requesting and perhaps non-existent addresses (page 2, para. 3-6). CERT Advisory teaches combating such attacks by reducing the likelihood that a particular network will be misused as the source of a SYN flooding attack. In particular, CERT Advisory teaches reducing the number of IP-spoofed packets entering and exiting a network.

CERT Advisory further teaches two principal methods for minimizing the risk of a SYN flooding attack originating from a particular network. First, CERT Advisory teaches a combination of: (1) filtering incoming packets that have a purported source address from within the network, and (2) filtering outgoing packets that have a purported source address different from the network (pages 3 and 4 APPENDIX A –REDUCING IP SPOOFED PACKETS, para. 2 and 3). Second, for routers that do not support filtering on the inbound side of an interface, CERT Advisory teaches using a second router between the external interface and the outside connection configured to block (on the outgoing interface connected to the original router) all packets having a source address within the internal network (page 4 ALTERNATIVE FOR ROUTERS THAT DO NOT SUPPORT FILTERING ON THE INBOUND SIDE, para. 1).

In contrast, Claim 1 recites a system for negotiating multi-path connections between a plurality of intermediary devices in a networked computing environment, comprising a client-side network protocol stack defined on an intermediary device available from a plurality of intermediary devices on a primary communications channel and establishing a client-side connection between a requesting client and the intermediary device in accordance with a connection-oriented network protocol. Claim 1 further recites a server-side network protocol stack establishing a server-side connection between the intermediary device and the requested server on a primary communications channel in accordance with the connection-oriented network protocol. Finally, Claim 1 recites a synchronization module determining differences in connection parameters defined for the client-side connection and the server-side connection

and communicating the connection parameter differences to at least one other such intermediary device over an out-of-band communications channel.

In contrast, Claim 7 recites a method for negotiating multi-path connections between a plurality of intermediary devices in a networked computing environment, comprising establishing a client-side connection between a requesting client and an intermediary device available from a plurality of intermediary devices on a primary communications channel in accordance with a connection-oriented network protocol. Claim 7 further recites establishing a server-side connection between the intermediary device and the requested server on a primary communications channel in accordance with the connection-oriented network protocol and determining differences in connection parameters defined for the client-side connection and the server-side connection. Finally, Claim 7 recites communicating the connection parameter differences to at least one other such intermediary device over an out-of-band communications channel.

Huegen fails to provide a suggestion or motivation to modify or combine with the reference teachings of CERT Advisory. Huegen addresses the problem of "smurf" and "fraggle" attacks where ICMP echo requests form the basis of the attack and the spoofed address is the address of the intended attack target. The effectiveness of the attack is conditioned on the availability of the directed broadcast function provided by poorly configured routers. Huegen proposes reducing the effectiveness of such attacks by removing this capability from the routers and limiting the rate at which echo packets can enter a network. CERT Advisory, on the other hand, addresses the problem of SYN flooding attacks wherein the target of the attack is the host itself and the spoofed address is intended merely to direct the SYN-ACK messages to destinations other than the true source of the SYN request. SYN flooding attacks of the type addressed by CERT Advisory make no use of the directed broadcast feature essential in both "smurf" and "fraggle" attacks. Although Huegen identifies SYN flooding as a denial of service attack "worthy of mention," Huegen teaches only that older TCP implementations are susceptible to attack and that a committed access rate ("CAR") can be used to limit TCP SYN flooding to particular hosts. CERT

Advisory discloses techniques aimed only at minimizing the likelihood of and effectiveness of SYN flooding attacks and teaches rejecting packets having suspect addresses, that is, incoming source address same as internal network, or outgoing source address different than originating network. CERT Advisory further teaches that, should the existing vendor's router not support suspect packet rejection, a second router could be used between the external interface and the outside connection. Thus, Huegen and CERT Advisory address distinctly different problems and achieve solutions using markedly different techniques. As a result, one of ordinary skill in the art would not find a suggestion or motivation to combine the teachings of Huegen with the teachings of CERT Advisory.

Similarly, one of ordinary skill in the art would not have a reasonable expectation of success in combining the teachings of Huegen and CERT Advisory. Disabling the directed broadcast feature as proposed by Huegen would not prevent a SYN flooding attack on a particular host because the success of such an attack does not depend on using such a feature to multiply the number of requests received by a host. Nor would use of a CAR as taught by Huegen defeat the effectiveness of a SYN flood attack on a particular host. The effectiveness of a SYN flood attack rests on the time wasted by a target victim waiting for ACK messages that never come rather than on the sheer volume of echoes received by the target victim. Similarly, CERT Advisory itself acknowledges that using the proposed filtering technique "will not stop all TCP SYN attacks, since outside attackers can spoof packets from any outside network, and internal attackers can still send attacks spoofing internal addresses." Thus, combining the teachings of Huegen and CERT Advisory would not result in a successful combination.

Finally, the combined references of Huegen and CERT Advisory fail to teach or suggest all claim limitations. Neither Huegen nor CERT Advisory teach determining differences in connection parameters defined for the client-side connection and the server-side connection and communicating the connection parameter differences to at least one other such intermediary device over an out-of-band communications channel, as recited by Claims 1 and 7. Huegen fails to teach or suggest connection parameter differences and, accordingly, fails to teach

or suggest determining such connection parameter differences or handling such connection parameter differences after the differences are determined. Again, Huegen teaches combating "smurf" and "fraggle" attacks by disabling the directed broadcast feature and limiting certain types of traffic to specific sources or destinations, not by communicating connection parameter differences among intermediary devices. CERT Advisory teaches only that an additional router can be used between an external interface and an outside connection and can be configured to block entry into the protected network of packets having a source address from within the network. CERT Advisory thus teaches a blocking system where packets having suspected spoofed addresses are blocked. In CERT Advisory, such addresses are suspected of being spoofed where incoming packets have a source address that is the same as the network address. CERT Advisory, therefore, does not rely on differences in connection parameters but, rather, on similarities between the source address and the network address. CERT Advisory fails to teach or suggest communicating any such connection parameter differences to another such intermediary device, as recited by Claims 1 and 7. CERT Advisory also fails to teach or suggest performing any such communication over an out-of-band communications channel, as further recited by Claims 1 and 7. Thus, the combined references of Huegen and CERT Advisory fail to teach or suggest all claim limitations.

Thus, a *prima facie* case of obviousness has not been shown with respect to Claims 1 and 7. Claims 2-6 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 8-11 are dependent on Claim 7 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 1-11 for obviousness under 35 U.S.C. §103(a) is requested.

Claim 12 stands rejected under 35 U.S.C. §103(a) as being obvious over Huegen, CERT Advisory Advisory, further in view of U.S. Patent No. 6,725,378, issued to Schuba et al. ("Schuba"). Applicant traverses the rejection. A *prima facie* case of obviousness has not been shown.

Claim 12 is dependent on Claim 7 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown with respect to Claim 7, withdrawal of the rejection of Claim 12 for obviousness under 35 U.S.C. §103(a) is requested.

Claims 13-19 stand rejected under 35 U.S.C. §103(a) as being obvious over Huegen, in view of U.S. Patent No. 6,697,872, issued to Moberg et al. ("Moberg"). Applicant traverses the rejection. A *prima facie* case of obviousness has not been shown with respect to Claims 13 and 17.

Moberg discloses a method for processing packets using encapsulation and decapsulation chains (Title). Moberg addresses the problem of enabling packets to travel through various networks having different packet handling protocols (Col. 5, lines 24-35). Moberg discloses that, encapsulation is required because at least one of the paths followed by the packet passes through a network that is not capable in the protocol used by the sender (Col. 5, lines 35-38). Moberg generally describes decapsulation as the process of stripping of a packet header and encapsulation as the process of prepending the packet with a new header (Col. 5, lines 45-51). Moberg further discloses performing these functions using both a primary processor, that is, a route processor, and a secondary processor, that is, a line card processor, and accomplishing both the decapsulation and encapsulation processes using decapsulation and encapsulation chains (Col. 5, line 66 – Col. 6, line 31). As each element in a chain has no specific knowledge of other elements in the chain, the chains can be modified without changing the existing elements. This process allows new features to be introduced to a router without changing existing code (Col. 6, lines 32-42).

Huegen and Moberg each fail to provide a suggestion or motivation to modify or combine their respective teachings. Huegen combats "smurf" and "fraggle" attacks by disabling the directed broadcast feature of a network that can be used by unauthorized users to direct an attack to a target outside the network. Huegen fails to teach or suggest any need for, or reason to, encapsulate packets. Similarly, Moberg fails to address any form of denial of service or other attack on

computer networks by malicious outside operators or agents. Moberg's teachings are confined to techniques for decapsulating and encapsulating packets and, more particularly, utilizing primary and secondary processors to perform these functions using a chain technique. Given that neither Huegen nor Moberg contains any teaching or suggestion as to why encapsulation has any role to play in combating "smurf" or "fraggle" attacks, one of ordinary skill in the art would not find a suggestion or motivation to combine the teachings of Moberg with the teachings of Huegen.

Similarly, one of ordinary skill in the art would not have a reasonable expectation of success in combining the teachings of Huegen and Moberg. Simply encapsulating packets to enable them to pass through networks employing different protocols would have no effect on whether those packets are effective at minimizing the effects of a "smurf" or "fraggle" attack. If the directed broadcast feature is disabled, as taught by Huegen, this disablement alone would be effective to thwart the effect of any such attempted attack, regardless of whether the packets are encapsulated. Encapsulation thus becomes superfluous as a means of combating such an attack. Combining the teachings of Huegen and Moberg would, therefore, not result in a successful combination.

Finally, the combined references of Huegen and Moberg fail to teach or suggest all claim limitations. Huegen fails to teach receiving a session packet on one of a plurality of link layer intermediary devices and receiving an echo response packet on at least one *other* link layer intermediary device, as recited by Claims 13 and 17. Huegen fails to teach multiple intermediary devices. Huegen also fails to teach using one intermediary device to receive a session packet and forward an echo request packet to a requested server, while using at least one other such intermediary device to receiving an echo response packet from the requested server and forwarding a response packet to a requesting client. As Huegen fails to teach multiple intermediary devices, Huegen fails to teach or suggest how such intermediary devices interact. More specifically, Huegen contains no teaching or suggestion that *different* such devices receive session and echo response packets, respectively, as recited by Claims 13 and 17. Instead,

Huegen discloses a single routing device that performs the directed broadcast function Huegen disables to avoid "smurf" and "fraggle" attacks.

Nor is any such teaching or suggestion found in Moberg. In particular, Moberg also fails to teach a plurality of link layer intermediary devices and fails to teach or suggest a system employing such devices where one intermediary device receives session packets and forwards echo request packets to a server, while another intermediary device receives an echo response packet from the server and forwards a response packet to the requesting client.

Claims 14-16 are dependent on Claim 13 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 18-19 are dependent on Claim 17 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown, withdrawal of the rejection of Claims 13-19 for obviousness under 35 U.S.C. §103(a) is requested.

Claim 20 stands rejected under 35 U.S.C. §103(a) as being obvious over Huegen, Moberg, and further in view of Schuba. Applicant traverses the rejection. A *prima facie* case of obviousness has not been shown.

Claim 20 is dependent on Claim 17 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. As a *prima facie* case of obviousness has not been shown with respect to Claim 17, withdrawal of the rejection of Claim 20 for obviousness under 35 U.S.C. §103(a) is requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Claims 1-20 are believed to be in a condition for allowance. Entry of the foregoing amendment is requested and a Notice of Allowance is earnestly solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: August 25, 2004

By: _____
Patrick J.S. Inouye, Esq.
Reg. No. 40,297

Law Offices of Patrick J.S. Inouye
810 Third Ave, Suite 258
Seattle, WA 98104

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

Figure 2.